ORIGINAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

SUSAN FLORENCE, On Behalf of Herself and All Others Similarly Situated,

Plaintiff,

vs.

JETBLUE AIRWAYS CORPORATION AND TORCH CONCEPTS, INC.,

Defendants.

CV 03 4847

Civil Action No.

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

CLASS ACTION COMPLAINT

BROOKLYN OFFICE

JURY TRIAL DEMANDED

AMON, J.

Plaintiff, Susan Florence, by her undersigned counsel, for her Class Action Complaint, alleges the claims set forth herein. Plaintiff's claims as to herself and her own actions, as set forth in ¶ 9 herein, are based upon her personal knowledge. All other allegations are based upon information and belief pursuant to the investigations of counsel. Based upon such investigation, Plaintiff believes that substantial evidentiary support exists for the allegations herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and/or discovery.

NATURE OF THE ACTION

1. This is a privacy class action lawsuit brought under the Electronic Communications Privacy Act - Stored Electronic Communications ("ECPA"), 18 U.S.C. § 2701 *et seq.*, state and common law. On or about September 19, 2003, Defendant JetBlue Airways Corporation ("JetBlue") announced that in September, 2002 it gave five million electronically stored passenger names, addresses, phone numbers and itineraries containing highly confidential personal information to a federal government contractor, Torch Concepts, Inc. ("Torch") (a data mining company), in violation of its own privacy policy as well as federal, state and common

law. Consumers have a legally protected privacy interest in their personal data and had an actual and reasonable expectation that Defendants would not transfer and/or use such information absent a customer's prior authorization and/or beyond a customer's consent.

2. Plaintiff brings this class action lawsuit on her own behalf and on behalf of a class of persons defined as:

> All persons in the United States who provided personally identifiable information to JetBlue Airways Corporation, prior to September, 2002 (the "Class Period"), and whose information has been transferred to or accessed by another person or entity absent the authorization and/or beyond the consent of the customer (the "Class").

3. Plaintiff alleges that Defendants have covertly, absent prior authorization and/or beyond the consent of herself and members of the Class, engaged in the surreptitious and unauthorized practice of, *inter alia*, transferring and/or accessing stored electronic information concerning Plaintiff and members of the Class.

4. By secretly transferring and accessing customers' electronically stored highly confidential, personal information, Defendants engaged in conduct that constitutes a serious invasion of privacy and trespass to property that is highly offensive in violation of federal, state and common law.

5. As a result of Defendants' wrongful course of conduct, Plaintiff seeks injunctive relief and monetary damages, including punitive damages, to redress Defendants' unlawful practice of secretly transferring or accessing millions of consumers' electronically stored personally identifiable information without their authorization and/or beyond their consent.

JURISDICTION AND VENUE

6. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. §§1331; 18 U.S.C. §2701, *et seq.* (Electronic Communications Privacy Act – Stored Electronic

Communications). This Court also has supplemental jurisdiction pursuant to 28 U.S.C. §1367(a).

7. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Defendant JetBlue maintains its principal place of business in this District and/or at all times conducted substantial business in this District.

8. In connection with the acts, transactions and conduct alleged herein, Defendants used the means and instrumentalities of interstate commerce, including the United States' mails and interstate telephone communication.

PARTIES

9. Susan Florence, a citizen of the State of New York, brings this action on behalf of herself and all others similarly situated. Susan Florence conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue.

10. JetBlue Airways Corporation ("JetBlue") is a Delaware corporation with its principal place of business located at 118-29 Queens Boulevard, Forest Hills, New York 11375. JetBlue, the eleventh largest passenger carrier in the United States based upon revenue passenger miles for the year ended December 31, 2002, is a low-fare, low cost passenger airline that began providing customer service on point-to-point routes in February, 2000. JetBlue has flown at least ten million passengers since commencing its operations. JetBlue had netcome of $54.9 million and $38.5 million for the years ended December 31, 2002 and 2001 respectively.

11. Torch Concepts ("Torch") is a Delaware corporation with its principal place of business located at 4650 Whitesburgh Drive, Suite 101, Huntsville, Alabama 35802. Torch is a leader in advanced technology for content management and information mining.

CLASS ACTION ALLEGATIONS

12. Plaintiff brings this action as a class action, pursuant to Fed R. Civ. P. 23, individually and on behalf of a Class as defined above. Excluded from the Class are the Court and its staff, Defendants, any parent, subsidiary or affiliate of Defendants and all officers and directors who are or have been employed by Defendants during the Class Period.

13. The Class is so numerous and geographically dispersed that joinder of all members is impracticable. While the exact number and identity of Class members cannot be ascertained by Plaintiffs at this time, it consists of the approximately five million JetBlue customers nationwide who submitted personally identifiable information to JetBlue that it stored electronically and unlawfully transferred to Torch.

14. The number of potential members of the Class is not precisely determined at the present time, but can be established through notice and discovery. The disposition of the Class' claims in this action will substantially benefit both the parties and the Court. The numerosity requirement of Rule 23(a)(1) is therefore satisfied.

15. Rule 23(a)(2) and Rule 23(b) are satisfied because there are questions of law and fact common to plaintiff and the Class, which common questions predominate over any individual questions affecting only individual members. Among these common questions of law and fact are:

(a) Whether Defendants participated in and/or committed or are responsible for the conduct complained of;

(b) Whether Defendants' conduct constitutes the violations of law alleged herein;

(c) Whether Defendants devised and deployed a scheme or artifice to defraud or conceal from Plaintiff and the Class members Defendants' practice of transferring and/or

accessing personally identifiable information without their prior authorization or beyond their consent;

(d) Whether Defendants engaged in deceptive acts and practices in connection with its undisclosed and systemic practice of transferring and/or accessing Plaintiff's and Class member's electronically stored personally identifiable information;

(e) Whether Defendants, through their wrongful course of conduct described herein, violated the Electronic Communications Privacy Act – Stored Electronic Communications, 18 U.S.C. §2701, *et seq.*;

(f) Whether the laws of the State of New York, and to the extent applicable, substantially similar laws of other states, were violated by Defendants, by engaging in the wrongful and deceptive practices alleged herein;

(g) Whether Defendants conduct was willful and/or intentional;

(h) Whether Defendants were unjustly enriched as a result of their wrongful course of conduct as alleged herein;

(i) Whether Plaintiff and members of the Class have sustained and/or are entitled to damages or are entitled to restitution as a result of Defendants' wrongdoing and, if so, the proper measure and appropriate formula to be applied in determining such damages and restitution;

(j) Whether Plaintiff and the Class are entitled to an award of statutory damages, compensatory and/or punitive damages; and

(k) Whether Plaintiffs and the Class are entitled to declaratory, injunctive, and/or other equitable relief.

16. In satisfaction of Rule 23(a)(3), plaintiff's claims are typical of the Class members' claims and do not conflict with the interests of any other members of the Class in that Plaintiff and the Class have all suffered from the same wrongful acts of the Defendants, namely, having their personally identifiable electronic information surreptitiously and without their authorization or beyond their consent transferred and/or accessed by Defendants. Plaintiff asserts claims that are typical of the claims of the entire Class, all Class members have been subjected to this same wrongful conduct, and the relief Plaintiff seeks is common to the Class.

17. In satisfaction of Fed. R. Civ. P. 23(a)(4), Plaintiff will fairly and adequately protect the interests of the other Class members and has no interests that are antagonistic to or which irreconcilably conflict with those of other Class members. Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in litigation of this nature to represent her and the Class.

18. A class action is the superior method for the fair and efficient adjudication of this controversy, since joinder of all Class members is impracticable. Plaintiff is not aware of any potential difficulties in the management of this action as a class action. Furthermore, because the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it prohibitively expensive for Class members to individually redress the wrongs done to them. Thus, because of the nature of the individual Class members' claims in this litigation, few, if any, could otherwise afford to seek legal redress against Defendants for the wrongs complained of herein, and a representative class action is therefore both the appropriate vehicle by which to adjudicate these claims and is essential to the interests of justice.

19. Absent a representative class action, Class members would continue to suffer losses for which they would have no remedy and Defendants would unjustly retain both the

proceeds of their ill-gotten gains and the wrongfully transferred/obtained data. Even if separate actions could be brought by individual Class members, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications which might as a practical matter be dispositive of the interests of the other Class members who are not parties to the adjudications, may substantially impede their ability to protect their interests and/or which would establish incompatible standards of conduct for defendants, making certification appropriate under Fed. R. Civ. P. 23(b)(1).

20. Pursuant to Fed. R. Civ. P. 23(b)(2), Defendants have acted and/or refused to act on grounds generally applicable to Plaintiffs and the Class, thereby rendering Class certification and injunctive and/or declaratory relief with respect to the Class as a whole pursuant to this sub-section appropriate as well.

21. A class action regarding the issues in this case creates no problems of manageability. In particular, notice of pendency of this action can be given in a variety of ways, including publication through the Internet and other media.

FACTUAL ALLEGATIONS

22. JetBlue is no stranger to controversy over possible invasions of passenger privacy, despite its public assurances to the contrary. In an article in *Aviation Daily* dated September 10, 2002, it was reported that certain airlines, including JetBlue, had surreptitiously placed video surveillance systems in the passenger cabins of its airplanes. Tom Anderson of JetBlue admitted his company was using such surveillance cameras to view passengers during flight, but claimed JetBlue had no plan to store the images obtained and that passengers (to they extent they knew about it) had not complained. In addition, in December 2002 the U.S. Transportation Security Agency ("TSA") announced that, in cooperation with JetBlue, it was dispensing with the usual

intrusive personal gate searches, but rather would engage in "enhanced security screening procedures" at the primary security checkpoint. JetBlue failed to elaborate what those "enhanced" measures were.

23. Since privacy is of paramount importance to consumers, JetBlue maintains on its website a clear privacy policy in a claimed effort "to demonstrate our firm commitment to privacy." According to this policy, JetBlue only uses computer IP addresses to help diagnose server problems, uses cookies to save consumers' name and e-mail so they do not need to re-enter such data, and uses optional passenger contact information solely for limited purposes: "to send the user updates and offers from JetBlue."

24. JetBlue specifically represents that any ticket information collected by JetBlue "**is not shared with any third parties, and is protected by secure servers,**" and also claims to have in place security measures to protect against the loss, **misuse** and alteration of consumer information under JetBlue's control. Moreover, as to children, JetBlue specifically represents that **it does not seek data from children and does not distribute to third parties any personally identifiable information about children without prior parental consent.**

25. Despite these public assurances that created a duty on the part of JetBlue to persons with whom it did business not to act in derogation of that policy, in September 2002 – at the same time it decided to implement the undefined "enhanced" security measures referred to above – JetBlue turned over to Torch Concepts as part of a taxpayer-funded study for which Torch Concepts received compensation JetBlue's Airline Passenger and Reservation database, containing the personal information of approximately 5 million of its customers that had flown JetBlue prior to that date – presumably without distinguishing between adults and children. This database contained passenger names, addresses, and telephone numbers. Also, while JetBlue has

not expressly admitted to this, the reservations data base contained information regarding Class members' itineraries so that Torch Concepts could analyze passenger traffic patterns, and possibly contained other information.

26. All of this personal information of Class members was stored in temporary, intermediate computer storage within JetBlue's servers since JetBlue takes a significant number of its reservations directly either over the Internet or through the phone, and such data is entered and stored in such servers. Through its extensive use of the Internet to run its business, JetBlue effectively operates an electronic communications service with such customers. Yet prior to turning over such data, JetBlue failed to obtain the consent of Class members to permit it to turn over such data for profiling testing or any other purpose.

27. While admitting on or about September 17, 2003 that it violated the rights of privacy of approximately 5 million class members, JetBlue claims it did so without compensation in a voluntary effort to assist with a government project regarding military base security. If this were the case, such conduct by JetBlue may have been in violation of both federal and state law, since a defense contractor that sets up a private records system may need to issue official notice of that system, which did not take place here. But more significantly, this explanation appears implausible in light of the lack of any apparent correlation between such passenger data and military base security, and co-defendant Torch Concepts claims otherwise.

28. In a February 25, 2003 report entitled "Homeland Security Airline Passenger Risk Assessment", prepared by Torch Concepts and publicly disclosed at a seminar conducted by the Tennessee Valley Chapter of the National Defense Industrial Association, Torch claims that it made initial overtures to obtain passenger data for this particular study from in December 2001 from various airlines. After receiving funding for conducting a passenger screening study in

March 2002, Torch claims that in July 2002 it was "given assurance that we would receive the necessary data base being used by CAPPS II contractors in weeks" (by way of background, CAPPS II stands for the Computer Assisted Passenger Prescreening System, a controversial air passenger profiling system in the testing stage but being opposed by numerous privacy advocates). The "CAPPS II contractor" was apparently JetBlue, despite the fact JetBlue's Chief Executive Officer, David Neeleman, has claimed JetBlue is not participating in CAPS II.

29. Moreover, according to published reports on or about September 15, 2003, the TSA had previously informed privacy advocates that JetBlue had given assurances to the TSA that it would help in the testing of CAPPS II.

30. In August 2002, Torch was informed (presumably by the TSA) that it would be receiving JetBlue's data base of customers for prior to September 2002, and in September 2002 actually received the JetBlue data base. Despite a later representation by JetBlue officials that "no data files were ever shared with the Department of Defense or any other government agency or contractor" and that it had provided such data to Torch over a year before this revelation, Torch claims to have received government funding for its passenger risk assessment project in March 2002 and the JetBlue data in connection with that particular project in September 2002.

31. If Torch had previously received this data over a year before September 2003 in connection with another project, there would have been no reason for the TSA to claim to have "facilitated" the transfer of such data as part of this project in August 2002 (although the TSA now claims to have had no role in the project and that it was not conducted under its auspices).

32. Moreover, if JetBlue was going to take such extraordinary actions in express derogation of its privacy policy, it must have placed express limitations on such data's use or

understood precisely what the data was to be used for – which if this aspect of JetBlue's story is to be believed, was not the case.

33. In October 2002, based on the massive data base it had received from JetBlue, Torch Concepts purchased data from a data aggregation company, Acxiom, Inc., containing detailed passenger demographic information. That data was then "merged" to create a mega data base of JetBlue passenger information - name, address, gender, own or rent a home, years at residence, economic status, number of adults and children in family, social security number, occupation and number of vehicles owned or leased.

34. Based on the data it received as part of its agreement with JetBlue, Torch Concepts was thereby able to gather detailed demographic data for over 2 million passengers, or 40% of the entire JetBlue data base. Torch Concepts then engaged in a data analysis for 200,000 "sample" passengers, grouped into "Younger Affluent" and "Older Affluent" categories, to determine JetBlue's passenger median age, income, length of residence, home ownership status, gender, adults, and children in family and social security number grouping.

35. As a result, with the active assistance of and/or agreement from JetBlue, Torch Concepts was able to create an unprecedented customer profiling scheme to "demonstrate that airline passenger and reservation data can be clustered to form groups of conventional travelers" and then show how this type of characterization, when extended to a more complete data base, can be used to identify "high risk passengers" who would be tagged yellow or red (and thereby subject to either higher pre-flight airlines checks or detention) to "distinguish normal JetBlue passengers from past terrorists" based solely on data attributable to "erroneous entry, fraud or mischief."

36. As an example of the type of data it had managed to gather, Torch Concepts publicly disclosed the personal details of what it characterized as "anomalous customer data" for at least one passenger, which was then made available on the Internet – where it remains accessible today, contrary to JetBlue's claims to the controversy.

37. In an ominous Orwellian statement, Torch Concepts concluded that its profiling system was workable and that with two additional elements that would require even more intrusive profiling (miles flown annually and lifetime) it would be able to "identify and characterize all normal travel patterns" and develop "passenger stability indicators" to assist in the passenger profiling process.

38. In the days since these revelations of wrongdoing began to be reported, JetBlue has admitted it made a "mistake" but tried to publicly obfuscate its role in this controversy. First, in an interview published on or about September 17, 2003, JetBlue cryptically admitted that "we clearly have to review internally this decision and reconsider our policies" in light of this admittedly embarrassing disclosure (not revealing which of its policies it needed to reconsider), but claimed that no customer information "has been provided for purposes of testing the CAPPSII program currently under design."

39. In light of the above statements made by the TSA about JetBlue's involvement in CAPPS II, this statement is of dubious accuracy. It is also misleading because the Torch Concepts analysis may not have been directly part of CAPPS II, but still tested a computer assisted passenger profiling system of some form utilizing massive computer profiling of class members that at least looks like a CAPPS II prototype.

40. Second, on or about September 18, 2003, JetBlue began to send e-mails to angry class members signed by Mr. Neeleman in an attempt to distance itself from the controversy and

"set the record straight". JetBlue represented that it has never supplied data to the TSA "or any other government agency" for CAPPS II "or for any other purpose whatsoever." Yet the TSA's spokesperson Brian Turmail has stated the TSA facilitated the transfer of JetBlue data to its contractor for a project that is apparently analogous to the mechanism that will be used in CAPPS II, thus at a minimum making JetBlue's statement misleading for want of disclosing material facts. Moreover, unless JetBlue agrees this data was misappropriated, it did in fact voluntarily turn over personal JetBlue passenger data to a TSA contractor for at least some purpose.

41. JetBlue also claims that the project had no connection with CAPPS II or aviation security, despite the express statement in the Torch study that its objective was to show how by "characterizing" passengers such an aggregation analysis "can be used to identify high risk passengers." JetBlue also asserts "no data files were ever shared with the Department of Defense or any other government agency or contractor". Yet JetBlue admitted turning over private passenger name, address and itinerary information obtained from its website and kept in storage on its own computer system, and transferred such data either directly or indirectly to Torch Concepts in electronic format. JetBlue apparently is using its own undisclosed definition of a "data file".

42. In a stunning admission, JetBlue also asserted in this apologetic e-mail that the presentation made by Torch Concepts was done "without JetBlue's knowledge." According to JetBlue, it had only responded to a request from the Department of Defense to voluntarily assist Torch Concepts with a project regarding military base security - a project that had no connection to either aviation security or the CAPPS II program. If JetBlue is to be believed, at a minimum Torch Concepts exceeded its authorization for the use of personal confidential customer

information supplied by JetBlue, in violation of federal, state and common law. And while Jet Blue attempts to take solace in the fact customer names were not disclosed, the information made publicly available was of such a detailed nature that for a few dollars or a few minutes of time, the names of passengers could be easily obtained. And JetBlue cannot hide from the fact such data was revealed to an unrelated third party.

43. Finally, JetBlue also claimed the sole set of data generated by Torch Concepts "has been destroyed" and that JetBlue is making "every effort" to have the Torch presentation removed form the Internet." Yet according to Torch Concept's lawyer Richard Marsden, as of September 17, 2003 Torch "still had the airline data" and was "in the process" of destroying it. Thus, it appears this data is still available for access, and absent court intervention there are no limits as to what will be done with such data and the database can be recreated. And the report summarizing such data is now distributed throughout the Internet and, absent monumental effort, cannot be eliminated.

44. While JetBlue claims it is "committed to making this right" and take steps to ensure such disclosures will not happen again, Defendants continue to mislead Class members as to the true facts and have failed to offer any compensation for these clear and admitted violations of privacy, despite the statutory mandates set forth below.

COUNT I

(Violation Of The Electronic Communications Privacy Act – Stored Electronic Communications, 18 U.S.C. §2701, *et seq.*)

45. Plaintiff repeats and realleges the allegations contained in Paragraphs 1-44 above, as if fully set forth herein.

46. Each instance of Defendants' wrongful course of conduct, as set forth above, constitutes a violation of the Electronic Communications Privacy Act, 18 U.S.C. §2701, *et seq.*,

in that Defendants, by and through their herein-described wrongful course of conduct, intentionally transferred and/or accessed without authorization and/or intentionally exceeded its authorization to access Plaintiff's and the Class members' electronically stored personally identifiable information and obtained access while in electronic storage and/or knowingly divulged the personally identifiable information while in electronic storage, all without or exceeding the knowledge, authorization, or consent of Plaintiff and the Class members.

47. Pursuant to 18 U.S.C. §2707, Plaintiff and the Class members are entitled to such preliminary or other equitable or declaratory relief as may be appropriate, at least $1,000 per Class member in statutory damages, actual and punitive damages, costs and reasonable attorneys' fees, plus disgorgement of any profits Defendants earned as a result of such violations of law.

COUNT II

(Trespass To Property)

48. Plaintiff repeats and realleges the allegations contained in Paragraphs 1-47 above, as if fully set forth herein.

49. As set forth in greater detail above, Defendants transferred and/or used Plaintiff's and the Class members' personal property, namely, their personally identifiable information contained in electronic storage.

50. Pursuant to the common law, Plaintiff and members of the Class are entitled to such preliminary or other equitable or declaratory relief as may be appropriate, compensatory damages, actual damages, including any profits made by Defendants and punitive damages.

COUNT III

(Invasion Of Privacy)

51. Plaintiff repeats and realleges the allegations contained in Paragraphs 1-50 above, as if fully set forth herein.

52. Defendants have, either directly or by aiding, abetting and/or conspiring to do so, knowingly disclosed, exploited, misappropriated and/or engaged in widespread commercial usage of private and sensitive information concerning the Plaintiff's and the Class members' personal affairs without the knowledge, authorization, or beyond the consent of Plaintiff and members of the Class. Such conduct constitutes a highly offensive and dangerous invasion of Plaintiff's and the Class members' privacy.

53. As Plaintiff and the Class members did not voluntarily authorize the disclosure of their personal and private information, such information was misappropriated.

54. As a direct and proximate result thereof, Plaintiff and members of the Class have been damaged by an amount according to proof at the time of trial and/or have been irreparably harmed by such conduct.

COUNT IV

(Unjust Enrichment)

55. Plaintiff repeats and realleges the allegations contained in Paragraphs 1-54 above, as if fully set forth herein.

56. Defendants have wrongfully and unlawfully enriched themselves to Plaintiff's and the Class members' detriment by engaging, and continuing to engage, in the above-described wrongful course of conduct for their own commercial benefit and enrichment.

57. Defendants' continued use, enjoyment, and retention of these wrongfully and unlawfully received funds violates fundamental principles of justice, equity, and good conscience and thus constitutes unjust enrichment.

58. As a direct and proximate result of defendants' above-described wrongful course of conduct, Plaintiffs and members of the Class are entitled to the relief set forth below, as appropriate.

COUNT V

(Declaratory Judgment)

59. Plaintiff repeats and realleges the allegations contained in Paragraphs 1-58 above, as if fully set forth herein.

60. Plaintiffs and the members of the Class members entitled to a declaratory judgment that by commission of the acts and omissions alleged herein, defendants have violated the Electronic Communications Privacy Act – Stored Electronic Communications, 18 U.S.C. §2701 *et seq.*, and/or Plaintiffs' and Class members' common law rights against trespass to property, invasion of privacy, and Defendants' unjust enrichment.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests that the Court enter judgment in his favor and against defendants:

(a) Determining that the action is a proper class action maintainable under Fed. R. Civ. P. 23; certifying an appropriate Class and certifying plaintiff as Class Representative;

(b) Ordering the temporary and preliminary off-site storage, under strict independent monitoring, of all information collected and/or shared as a result of Defendants'

wrongful conduct described herein in order to preserve the *status quo* pending the Court's resolution of the issues raised by this Complaint;

(c) Ordering a temporary and preliminary asset freeze or constructive trust on all monies wrongfully obtained, and all profits wrongfully derived, as a result of the conduct alleged in this Complaint in order to preserve the *status quo* pending the Court's resolution of the issues raised by this Complaint;

(d) Declaring the acts and practices complained of herein to be in violation of the statutory and common laws set forth above;

(e) Enjoining and restraining the Defendants from any further acts in violation of the statutory and common laws set forth above;

(f) Directing the Defendants to take such affirmative steps as are necessary to ensure both that the causes and effects of their unlawful information-handling acts and practices are eliminated and no longer continue and that all Class members are specifically notified of JetBlue's information-handling acts and practices and the existence and availability of a remedy to correct the illegal activities set forth above. At a minimum, such affirmative steps must include: (i) ordering the Defendants to conduct a corrective advertising and information campaign advising consumers whose electronically stored personal information has already been transferred and/or accessed how to determine if their information was improperly transferred and/or accessed, and (ii) ordering the destruction and/or purging, under court monitoring, of all personally identifiable information transferred by JetBlue to any person a result of Defendants' wrongful conduct described herein.

(g) Awarding Plaintiff and the Class any and all amounts owing to them under the statutes of the United States set forth above;

(h) Awarding Plaintiff and each Class member their actual and compensatory damages for violations of the statutes of the United States set forth above and violations of their right to be free from trespass to property, invasion of their privacy;

(i) Awarding Plaintiff and members of the Class punitive damages;

(j) Directing Defendants to disgorge all monies wrongfully obtained as a result of the conduct alleged in this Complaint and awarding to plaintiff and the Class members all profits derived or monies saved as a result of the unlawful acts and practices alleged herein;

(k) Awarding Plaintiff and the Class members the costs of this action, together with reasonable attorneys' fees;

(l) Awarding Plaintiff and members of the Class pre- and post-judgment interest; and

(m) Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, plaintiff hereby demands a trial by jury in this action of all issues so triable.

Dated: September 22, 2003
New York, New York

MILBERG WEISS BERSHAD HYNES & LERACH LLP

By: _____

David J. Bershad (DJB-9981)
Michael M. Buchman (MB-1172)
J. Douglas Richards (JDR-6038)
One Pennsylvania Plaza
New York, New York 10119-0165
Telephone: (212) 594-5300

Jack G. Fruchter
FRUCHTER & TWERSKY LLP
One Penn Plaza, Suite 1910
New York, New York 10119
Telephone: (212) 279-5050

Attorneys for Plaintiff